SUFFOLK COUNTY POLICE DEPARTMENT
IDENTITY THEFT UNIT

POLICE COMMISSIONER RICHARD DORMER

Fact:

- The emotional impact of identity theft is similar to that suffered by victims of violent crimes.
- Most identity theft is committed through traditional means such as lost or stolen wallets or purses, mail theft, or misappropriation of personal identifiers by family or friends.

How does it Happen?

- The victim gives out his/ her information to phone caller or mail request.
- Lost or Stolen wallets and pocketbooks.
- Stolen or Diverted Mail.
- Stolen Trash, known as “Dumpster Diving”.
- Burglary of residence or business.
- Credit Card “skimming”
- Unscrupulous Employees
- Internet
    - “Phishing”
        - “Phishing" is an e-mail message from that appears to be sent by a legitimate institution which attempts to trick consumers into revealing personal information—such as their credit or debit account numbers, checking account information, Social Security numbers, or banking account passwords—through fake Websites or in a reply e-mail.
    - Fake websites
        - Fake websites mimic the sites of established companies to trick prospective customers into revealing credit card information.
    - Unsecured wireless networks
        - As more people install wireless routers on their home networks they fail to utilize the security features on their wireless routers or firewall software. Criminal’s can gain access to a victims unsecured internet connection and use it to commit crimes and frauds.
    - Unsecured laptops using “hotspots”

- Criminals can gain access to your laptop while you use a public “hotspot” and obtain any personal or important information

What Crimes or Frauds can be Committed with Your Identity?

- Open cell phone and wireless service.
- Open new credit card accounts.
- Take over your existing credit card accounts.
- Open bank accounts.
- Counterfeit your checks and credit/debit cards.
- Buy cars and houses.
- Commit crimes in your name.

Prevention

- **Vigilance = Protection!**

- **Give yourself the choice!** Ask a merchant or service provider requesting your Social Security number or personal information;
    - Why do they need it?
    - What will they do with it?
    - Where will it be kept?
    - Will you still get the merchandise or service if you do not provide them your personal information?
    - Can you substitute passwords or identifiers of your choosing?
- **Wallet or Pocketbook**
    - Only carry the personal information you need daily in your wallet or purse.
    - Leave your **Social Security Card** in a safe place at home.
    - Reduce the number of credit cards you carry- Better yet only take a credit card with you when you expect to use it.
    - DO NOT keep copies of Social Security numbers, Account numbers, PINS or other identifying information in your wallet.
    - You must carry your drivers license and in many cases business or school identification as well as health insurance cards. Such documents may contain your **Social Security number**. If possible replace your Social Security number with a different identifying number or password.

- **Protect your mail.**
    - Locking mail boxes
    - Vacation hold
    - Outgoing mail to post office collection boxes
    - Remove your name from Direct Marketing Lists
    - Opt-Out of receiving pre-screened credit offers.
    - Know your billing cycles.
- **Shred** documents containing personal information before placing in trash.
- **Passwords** on credit, debit cards, bank and phone accounts.
- **Secure Your Information**
    - At home – burglar proof
    - Know who has access to your info such as Family, Friends and Home Assistants. Take action to secure your information from those who you do not want to have access.
- **Order Your Credit Bureau Reports**
    - Check your credit reports carefully for credit cards and loans you may not have opened or applied for.
- **Computer Security.**
    - Update your Operating System and virus software.
    - Use antivirus software.
    - Watch out for e-mail attachments.
    - Turn the computer off.
    - Use Firewall Software.
    - Use a strong password containing both large and lower case letters and numbers.
    - Use a router and keep security firmware updated.
- **Wireless Networks**
    - Make sure you change the default password
    - Change the default SSID- change it frequently
    - Enable Wireless Security
    - Disable SSID Broadcast
    - Keep the wireless router firmware updated
- **Laptop Computers**
    - If possible **DO NOT** store personal data on a laptop
    - Consider Physical security
        - Locks
        - Cables
    - Use bios and sign on Passwords
    - Enable Document encryption
- **Public Wireless Connections**
    - Keep software updated
    - Turn on XP Firewall or other software firewalls

    - Enable encryption which prevents “sniffing”
    - Never
        - send confidential info
        - use passwords
        - View online bank statements
    - Be aware of Rogue Access Points
- **Computer Hard Drives**
    - **DO NOT** discard old hard drives in the trash without first:
        - Using specialized disk wiping software to clear data from the hard drive
        - Destroy the hard drive if no longer needed

What to Do If You Become a Victim of Identity Theft.

IMMEDIATELY!

- Call the Police
    - Providing the credit bureau agencies with a copy of a police report will allow them to extend the fraud alert on your information to seven years.
- Contact the three major credit bureaus.
    - Place a fraud alert on your records.
    - Request your credit bureau reports.
    - Check your reports carefully, make sure you can identify every entry reported, close any accounts not opened by you.
- Call the creditors involved.
    - Advise them that you are the victim of Identity Theft
    - Close the affected accounts
- Correct the address for any mailings in your name being sent to the wrong location by contacting the U.S. Postal Inspectors.
- Contact the Federal Trade Commission Identity Theft Hotline
    - Phone: 1-877-IDTHEFT (438-4338)
    - TDD: 202-326-2502
    - Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington D.C. 20580
    - Online: www.consumer.gov/idtheft

Get Control of your Identifiers!

A few guidelines to regain control of your life and your financial well being by proving to financial institutions that you are the victim not the perpetrator.

- Gather all the information you possess regarding the theft and use of your personal identifiers.
- Chart a time line as to the sequence of events as you understand them. Correct the time line as you gather more information.
- Keep a diary and document any phone calls regarding your problem; record the date, time and the names of persons you called and what information was discussed. Get direct phone numbers of those contacted as well as addresses for future correspondence.
- Follow up all phone conversations with a written correspondence confirming the details of your conversation. Send the correspondence certified mail with a return receipt.
- Keep hard copies as well as computer copies of all correspondence, bills and charges either sent or received.
- Keep track of expenses related to correcting your personal identifiers or credit information for the possibility of future restitution.
- Stay organized, that may be difficult in such stressful circumstances so you may need to enlist a family member or close friend to assist you in the effort.

Resources:

Remove your name from Mailing or Call Lists

- Unsolicited Credit card Offers:
    - 1-888-5-OPTOUT (1-888-567-8688)
- Experian's Marketing Lists:
    - 1-800-407-1088
- Direct Marketers: The Direct Marketing Assoc.
    - Mail: Mail Preference Service
      Direct Marketing Association
      PO Box 643
      Carmel, NY 10512

    - www.the-dma.org

Credit Bureau Contact Numbers

Credit Bureau	Report Fraud	Credit Reports	Web Sites
Equifax	1-800-525-6285	1-800-685-1111	www.equifax.com
Experian	1-888-397-3742	1-888-397-3742	www.experian.com
Trans Union	1-800-680-7289	1-800-916-8800	www.tuc.com

Free Credit Bureau Reports once a year.

There are three ways to get them:

- Click on the Web site **www.annualcreditreport.com** and fill out a request.
- Call 877-322-8228.
- Print out the annual credit report request form at **www.ftc.gov/credit** and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

If you discover an error in a report, write the reporting company to explain the situation.

Social Security Administration Hotline:

- 1-800-269-0271
- www.socialsecurity.gov/oig

Mail Theft: Contact the U.S. Postal Inspectors

- www.usps.gov/websites/depart/inspect

Your name may be your greatest asset, keep it to yourself!

Suffolk County Police Department
Identity Theft Unit
30 Yaphank Ave.
Yaphank, NY 11980

Phone: 631-852-6821
FAX: 631-852-6820